The EU data protection regime and the multilateral trading system: Where dream and day unite

Gianpaolo Maria Ruotolo[*]

1. *Introduction*

> 'Fast forward a decade and imagine your morning routine.
> You wake up gently at a time carefully selected by a bracelet monitoring your sleep patterns after drawing on weeks of data stored on a server that lives somewhere in the American west.
> You trudge to the bathroom and step on to the scales, which quickly shoots your weight to that same server and helps determine just how long and how strenuous your next session on the treadmill will be. (…)
> Later, your toothbrush sends updates to a dental service and, spotting the early signs of a cavity, books an appointment.
> Welcome to the 'internet of things', now perplexing trade negotiators and experts on digital trade.
> Were you to live in Europe those sleep records stored on a US server could easily violate data localization and privacy laws. The same applies to the incriminating information shared by your bathroom scales. Your fridge and coffee pot might well be communicating via a server in South Korea or China, which in turn is liaising with a Google server in Ireland to check on your calendar. The first six months of your dental service came free with the Chinese-made toothbrush you bought at a local chemist but renewing it means paying your fees to the service in Germany that relays your data to a virtual clinic staffed by experts in Bangalore, who send your particulars to the local dentist.'[1]

We won't have to wait anymore.

[*] Università di Foggia – Dipartimento di Giurisprudenza; University of London – Institute for Advanced Legal Study (IALS).

[1] S Donnan, 'Digital Trade: Data Protectionism' *Financial Times* (5 August 2014) <www.ft.com>.

Massive collection of both personal and non-personal data is nowadays a fact all over the world.

This has led to the gathering of databases of enormous dimensions, built for the most varied purposes. Such data are gathered thorough the consensual conferment made by individuals and by automated means, through smart devices always connected to the Internet (the so-called Internet of Things, IoT), and even by objects with sensors to understand features of their environment and an ability to communicate (robots).

Data may ease and increase international trade, commercial exploitation of intellectual property rights, and even investments abroad: the way they are ruled is thus playing a pivotal role for economic operators, States and international organizations.

In this climate, the statement according to which the Internet – the main tool for the transferring of data – has shifted into the 'global market' is so frequently repeated by politicians, commentators, commercial operators and even by members of the scientific community[2] to have become a catchphrase devoid of any real content.

At a deeper look that catchphrase, indeed, englobes different phenomena any of which deserves an autonomous analysis, rather than an aggregate description.

The purpose of this paper is to isolate and study one of these phenomena: the way domestic regulatory frameworks protecting personal data relate to multilateral trade rules.

This will imply both to try and bridge information technology law (IT law) with international trade law and reviewing World Trade Organization's practice in the field of digital commerce.[3] This, as we shall see, may provide us with some elements to evaluate the impact of data

[2] See S A Aaronson, 'Trade and the Internet' (2012) Intl Economy 75; M Burri, T Cottier, 'Digital Technologies and International Trade Regulation', in M Burri, T Cottier (eds), *Trade Governance in the Digital Age* (CUP 2012) 3; F Erixon, B Hindley, H Lee-Makiyama, 'Protectionism On-line: Internet Censorship and International Trade Law' (2009) ECIPE Working Paper, Brussels, 12; J Meltzer, 'The Internet, Cross-Border Data Flows and International Trade' (2013) 22 Issues in Technology Innovation <www.brookings.edu/wp-content/uploads/2016/06/internet-data-and-trade-meltzer.pdf>.

[3] On a previous tentative of ours to try and bridge international law and IT law see GM Ruotolo, 'Fragments of Fragments. The Domain Name System Regulation: Global Law or Informalization of the International Legal Order?' (2017) 33 Computer L & Security Rev 159.

protection regimes on the multilateral trading system, and vice-versa. In the second part of the work we will try to apply some of these principles to the latest EU data protection rules as a case study.

The use of the Internet as a means for contacting customers, concluding contracts and, at least for some types of goods and services even delivering them, has allowed economic operators both to reduce their costs and having an opportunity to reach potential buyers physically far away, and for this previously unreachable. This increased competition and generated advantages for consumers too, for it increased the number of suppliers and lowered the prices of available goods and services. This significantly increased the volume of both business to business (B2B) and business to consumer (B2C) international online trade and become a tool of growth set free from territorial factors, and emancipation of peoples living in least developed areas of the world.

This highlighted the needs for a 'global' regulation.[4]

2. *Digital commerce in WTO as a context: a brief survey*

The sharing of personal data and their cross-border transfers are often essential to enable commercial transactions, especially (but not only) for the online ones.

One may think of the need to communicate the data of a credit card or other payment instruments, or the address of a person's residence, in order to fulfill a purchase order or, again, of the need to centralize the storage of emails or other data in order to improve the quality of a given service.

In other cases the very possibility of providing a specific service is conditioned by data transfers:[5] one may think of the need to process

[4] The resolution of the UN General Assembly of the 9th February 2010 on 'Information and communication technologies for development' (UN Doc A/RES/63/187) recognizes the Internet as a means of promoting the economic development of the least developed countries.

[5] This kind of data do not necessarily have to be referred to a specific individual, which leads to the issue of the non-personal data, that happens mostly in the case of the so-called Big Data, that need an autonomous analysis, we cannot lead here. On this issue, also for further bibliographic references, see G Della Morte, Big Data *e protezione internazionale dei diritti umani. Regole e conflitti*, (Editoriale Scientifica 2018) *passim*;

large databases related to the efficacy of a certain drug on a given disease in order to evaluate which therapy to take in a given case. Therefore, the impact on the multilateral trading system produced by the rules that regulate data, their treatment, and their international transfers have to be framed in the context of the digital trade.

The regulation of trade by digital means represents, even in the ongoing crisis of the last years, a pivotal issue of the agenda of the World Trade Organization (WTO).

Since its first years, the WTO Members, wide aware of the importance of some goods (such as personal computers, routers and the like) for the diffusion of information technologies, tried to liberalize the sector and signed the 1996 Information Technology Agreement (ITA),[6] which provides for the elimination of customs duties on hundreds of IT products, regardless of their method of purchase, be it analog or digital.

During the celebrations held for ITA's twentieth birthday, held in Geneva in June 2017, WTO Members discussed about the ITA and its expansion, decided two years before, during the 2015 Nairobi Ministerial Conference, in order to lead to the elimination of tariffs on two hundred products more.

Though ITA is just a tariff-cutting instrument, the debate focused mainly on non-tariff barriers and, in particular, on declarations of conformity, e-labeling,[7] and transparency. We must underline that transparency is one of the pillars of national and regional data protection regulations: for instance, Article 5 of the EU General Data Protection Regulation (GDPR) sets out a number of principles that data controllers must comply with when processing data, and imposes them to process all data 'lawfully, fairly and *in a transparent manner*'.[8]

GM Ruotolo, 'I dati non personali: l'emersione dei big data nel diritto dell'Unione europea' (2018)13 Studi sull'integrazione europea 97.

[6] *Ministerial Declaration on Trade in Information Technology Products* doc WT/MIN(96)/16 (13 December 1996).

[7] Physical labels on products, even still mandatory, are getting no longer fit for their purpose, as there are often too many marks to be put on products that are getting smaller and smaller: e-labelling – as QR codes – may be a smart solution, as they have no physical restrictions, can be updated throughout the life of the product, are more accessible and even greener.

[8] EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, as well as the free circulation of such data.

Furthermore, in line with decisions again taken by the 2015 Nairobi Ministerial Conference,[9] over the last two years, WTO General Council has examined the progresses made in negotiations on electronic commerce: the main proposals on which the WTO bodies[10] are working show that the Organization's Members are widely aware of the centrality of this issue in general, and of its data protections facets in particular, for the very survival of the WTO itself.

The negotiations, besides trying to regulate some substantive aspects of the digital commerce itself, aim at introducing in the multilateral trading system specific rules that prevent Members from adopting measures which could work as digital trade restrictions, even when they're not construed to directly regulate e-commerce.[11]

Under the first profile WTO Members are trying to turn the moratorium on digital commerce into a fully binding legal obligation.

The moratorium – originally adopted in 1998 and successively extended many times, at last by the 2017 Buenos Aires Ministerial Conference – is the political commitment of the Member States to exclude from the application of tariffs every digital product bought through electronic instruments and electronically delivered (the so-called 'liquid' goods, sold through 'direct' electronic commerce: one may think of the case of file downloads containing music, films, e-books, software, videogames, etc.).

Goods electronically purchased but physically delivered ('indirect' electronic commerce, which occurs in the case of the on-line purchasing of products that are then physically delivered) are instead subject to ordinary tariff regimes.[12]

[9] WT/MIN(15)/42 — WT/L/977.

[10] In addition to the General Council, in particular the Services' and TRIPs' Councils.

[11] JOB/GC/94 (US); JOB/GC/96 (Japan et al); JOB/GC/97 (EU et al); JOB/GC/98 (Brazil); JOB/GC/99 (MIKTA countries); JOB/GC/100 (Japan); JOB/GC/101/Rev.1 (Singapore et al); all the documents are downloadable at <www.wto.org>.

[12] WTO moratorium on the electronic commerce is an act void of binding effects, but not *tout court* of legal ones. In this sense can be read both its literal formulation, which asks Members to 'continue their current practice of not imposing customs duties on electronic transmissions (..) without prejudice to (…) the rights and obligations of Members under the WTO Agreements', and the type of act in which it is enshrined, a declaration of the Ministerial Conference. Although art IV, para 1 of the WTO Agreement gives the Ministerial Conference 'the authority to take decisions on all matters un-

On the other hand, that explicitly refers to transboundary data flows, some developed States proposed to introduce into the multilateral trading system obligations to impose Members to allow cross-border data flows. Those proposals are inspired by the idea that rules regulating data processing, especially those which restrict their transfer from one State to another, operate as non-tariff barriers, as the transfer itself, as we have already said, can choke international exchanges.

A look at the US practice shows that domestic regulations banning cross-border data flows are felt as 'a chokehold on the free flow of information, which stifles competition and disadvantages digital entrepreneurs'.[13] On this premise the US propose that 'appropriately crafted trade rules can combat such discriminatory barriers by protecting the movement of data, subject to reasonable safeguards like the protection of consumer data when exported'.[14] Linked to this proposal is the one which aims to prohibiting establishment obligations for data processing: the idea is to prevent States from imposing on those operators who rely on cloud computing for the provision of products and services, to build infrastructures and data centers in each Country they intend to serve; such localization requirements add unnecessary costs and burdens to both suppliers and consumers.

der any of the Multilateral Trade Agreements', some commentators have indeed supported a restrictive interpretation of all the provisions that allow the Ministerial Conference to adopt binding acts; see G Adinolfi, *L'Organizzazione mondiale del commercio. Profili istituzionali e normativi*, (CEDAM 2001) 133 ff. Moreover art X of the same WTO Agreement requires that any changes to the obligations WTO system imposes on Member States can enter into force only through the prior ratification of all of them, which, in the moratorium case, never occurred. Nor, again because of the absence of any ratification by the competent national bodies, it seems that the moratorium can be attributed the nature of a GATT tariff commitment: there is difference between the procedure for adopting the moratorium and the one used, for example, for the ITA, an international agreement, as we said earlier, entered into force only after reaching the requested number of ratifications. In essence, therefore, the moratorium has to be qualified as a recommendation by the Ministerial Conference to the States, which is in any case capable of producing at least the legal effect of obliging them to provide adequate reasons whenever they violate it.

[13] The US have the same approach, as we will see, in their bilateral trade negotiations: for instance, one may see the Trans-Pacific Partnership (TPP), chapter 11, Annex 11-B, section B and Chapter 14, art 11.

[14] See WTO doc JOB/GC/94 <www.wto.org>.

It should be said incidentally that, in this very regard, as we will see in section 5, the proposal is not far from the approach adopted in the EU GDPR.

This element of convergence surfaces after EU and US, in the past, showed distant approaches in terms of privacy and data protection: indeed, the Court of Justice of the EU overturned the Commission's decision 2000/520/EC of 26th July 2000 on the adequacy of the protection offered by the principles of safe harbor in the field of confidentiality published by the United States Department of Commerce, the so called *Safe Harbour*,[15] and that later EU and US signed the *Privacy Shield*.[16]

Both these instruments were adopted in the light of the so called *adequacy decisions* in application of Article 25 of the directive 95/46/EC of the European Parliament and of the Council, now substituted by Article 44 of the GDPR. We will examine the latter provision and its relationships with the WTO system in para 6 of this work.

3. *Transboundary data flows and exchanges of goods*

Let us now try to draw up some general guidelines to scrutiny the compatibility with the multilateral trading system of domestic measures regulating data processing and, in particular, of rules that limit or set up conditions for international data transfer, like the abovementioned Article 44 and Article 45 of the GDPR.

To do this we must first deal with a qualification issue, that is to say that we need to identify the applicable WTO rules.

[15] The decision was adopted in application of art 25 of the Directive 95/46/EC of the European Parliament and of the Council, now substituted by art 44 of the General Data Protection Regulation. We will examine deeper the latter provision in section 6 of this work.

[16] The EU-US Privacy Shield Frameworks was adopted on 12 July 2016 and became operational on 1 August 2016. It was drafted by the U.S. Department of Commerce and the European Commission to provide a mechanism to comply with data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. On July 12, 2016, the European Commission deemed the EU-US Privacy Shield Framework adequate to enable data transfers under EU law. We must remind that art 45 of the GDPR provides for the continuity of adequacy determinations made under the EU's 1995 data protection directive, one of which was just the adequacy decision on the EU-US Privacy Shield.

First of all, we have to try and understand whether and to what extent such regulations affect the system of trade in goods and, for this, they fall within the scope of GATT.

Transboundary (both personal and non-personal) data flows may impact on the application of many GATT rules, such as the national treatment (and in particular Article III, para 4), the principle of exclusive customs protection (Article XI, para 1), the general exceptions clause (set out in Article XX), the national security clause (Article XXI)[17] and furthermore, may affect the Agreements on customs valuation, licensing procedures and on rules of origin.

As one may easily see, most of those rules deal with non-tariff issues,[18] and this should not be a surprise, as the e-goods tariff issue is ruled by the moratorium we already spoke about.

Now, non-tariff obstacles are characterized by extreme heterogeneity and may be embodied in each and every State measure restrictive of trade and different from the imposition of customs duties: in the context we are dealing with, they take the form of measures aimed at blocking, restricting or placing conditions on international data flows.[19]

WTO dispute settlement practice has dealt with the trade impact of measures controlling and restricting Internet transmissions in the case of *China – Audiovisuals*.[20]

There, the United States contested China's violation of WTO obligations relating to the importation and distribution of goods and services pertaining to reading materials (books, newspapers, electronic

[17] Art XXI, as is well known, allows Member States to derogate from the obligations deriving from belonging to the multilateral trading system in order to pursue national security issues. The rule, in fact, could be highlighted in the case of threats implemented by computer. This is an issue, however, that is beyond the scope of this paper. See S Peng, 'Cybersecurity Threats and the WTO National Security Exceptions' (2015) 18 J Intl Economic L 449 and, with a wider approach M Finnemore, DB Hollis, 'Constructing Norms of Global Cybersecurity' (2016) 110 AJIL 425.

[18] P Malanczuk, Data, 'Transboundary Flow, International Protection' *Oxford Public International Law* <opil.ouplaw.com>.

[19] A Chander, UP Le, 'Breaking the Web: Data Localization vs. the Global Internet', (2014) University of California Davis School of Law, Legal Studies Research Paper Series <www.sssrn.com>.

[20] *China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Report of the Panel WT/DS363/R (12 august 2009) <www.wto.org>.

journals), audiovisuals products for home entertainment, sound recordings and movies intended for cinema projection.

Although the dispute dealt with measures restricting digital downloads and not explicitly with cross-border data flows in strict sense, it could provide us with some elements for assessing, in a multilateral trading system perspective, the data protection measures.

Article III GATT imposes on Members the national treatment obligation, in order to assure that imported products have a no less favorable treatment than the one foreseen for similar national products. In particular, Article III, para 4 prohibits discrimination with regard to internal measures other than taxation.

The WTO litigation practice, over the years, has clarified scope, functions and application mechanisms of these provisions.

The *Audiovisuals* case clarified that a violation via the Internet occurs in the presence of three conditions: that discrimination is between 'like products', that discriminatory measures are embodied in 'laws, regulations, or requirements that affect internal sale, offering for sale, purchase, transportation, distribution or use', and that imported products are applied a 'less favorable treatment' than the corresponding national products.

Regarding the first requirement, the *Audiovisuals* panel, to determine the status of digital products, referred to a well-established case law[21] and affirmed that the similarity between products can be identified on the basis of four criteria, such as '(i) the properties, nature and quality of the products; (ii) the end-uses of the products; (iii) consumers' tastes and habits – more comprehensively termed consumers' perceptions and behavior – in respect of the products; and (iv) the tariff classification of the products'. On those bases the panel declared the

[21] See *United States — Standards for Reformulated and Conventional Gasoline*, Report of the Panel WT/DS2/DS4/R (29 January 1996) para 6.8; *Japan – Taxes on Alcoholic Beverages*, Report of the Appellate body WT/DS8/DS10/DS11/AR/R (4 October 1996) 113 under note 46. One may also recall that the Appellate Body, in its report on the case *European Communities — Measures Affecting Asbestos and Products Containing Asbestos*, WT/DS135/AB/R (12 March 2001) affirmed that '"likeness" under Article III:4 of the GATT 1994 is fundamentally a determination about the nature and extent of a competitive relationship between and among products' para 99.

similarity of the digitally downloaded products with their traditional counterparts.[22]

The panel then proceeded to scrutinize the contested measures and ascertained that they aimed at verifying the content of the digital products in order to prevent the transmission of unwanted messages, even if the corresponding physical copy had already been imported. In the panel's opinion, therefore, the measures in question were applicable on the basis of 'an internal factor separate from importation' and they fell within the scope of application of Article III, para 4 GATT 1994.

Moreover, all the contested measures regulated also the ways in which digital goods 'may be distributed (such as subscription channels) and who may distribute them (ie, wholly state-owned enterprises)' and therefore negatively affected their diffusion and infringed Article III, para 4 of the GATT 1994.[23]

The panel also ruled on the applicability, to the disputed measures, of the general exception clause of Article XX GATT, which allows Member States to derogate from any GATT obligation to protect some superior interests (including public morals), but only if the derogating measures do not constitute 'a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade' (thus the chapeau of Article XX), they are necessary and produce the least possible impact on exchanges.

Also on this aspect the panel conclusions, later confirmed by the Appellate Body (AB), applied a settled case-law according to which the analysis regarding compliance with Article XX GATT must be conducted by a two-phase procedure aimed at 1) determining whether the disputed derogation measure falls within one of the provisions of the article and 2) if it complies with the requirements contained in the preamble thereto.

Furthermore, the requirement of necessity, in turn, is split into two elements: a principle of necessity in strict sense, relating to the indispensability of the measure adopted with respect to the purpose it pursued, and a wider principle of proportionality, which requires that the chosen

[22] *Audiovisuals* Panel Report (n 20) para 7.1445.
[23] *Audiovisuals* Panel Report (n 20) para 7.1522.

measure is, among those suitable to achieve the desired purpose, the one that produces the least restrictive effects of trade.[24]

On this point, in *Audiovisuals*, the AB recalled that it had already ruled that 'a necessary measure is located significantly closer to the pole of "indispensable" than to the opposite pole of simply "making a contribution to"':[25] the contested measures had therefore to be considered as infringing WTO obligations as there was no linkage between them 'and the protection of public morals measures as far as possible from the pole of indispensability to qualify as necessary within the meaning of Article XX'.[26]

There is to say that our quest for scrutinizing parameter could have obtained more elements of interest if the dispute had concerned the adoption of State measures slowing down or totally blocking the Internet data flows, as they could constitute a violation of Article XI, par. 1 GATT, but this was not the case.

As, in fact, the Internet is the main tool of delivery, its total or partial block (as could be a data transfer restriction measure) could represent a quantitative restriction comparable to a quota, even to a zero quota in the case of a total block.

So, State measures that impose to control the content of a digital data flow as a precondition for its entry into a national market, or that conditions the entry to an authorization of an administrative authority, are to be read as equivalent to a procedure for granting an import license, explicitly contemplated by Article XI GATT.

We have to keep this in mind while considering the EU Commission's adequacy decisions pursuant to Article 45 DPGR (below, section 6).

In a methodological perspective, the conclusions reached in *Audiovisuals* regarding the application of GATT Article III, para 4 and Article XX to digital products, widely use mechanisms and interpretative models well consolidated in the WTO practice concerning real life goods. This indicates that online situations do not *always* need *ad hoc*

[24] See *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, Report of the Appellate Body WT/DS363/AB/R (21 December 2009) para 415.

[25] *Korea — Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, Appellate Body Report WT/DS/1690/AB/R (11 December 2000) para 161.

[26] *Audiovisuals* Panel Report (n 20) para 4.211.

standards and they can be mostly regulated by means of general provisions, with some interpretative adjustments.

It must be said that some Authors contest this conclusion by highlighting that the WTO system has been unable to adapt to the needs of digital trade and data protection and therefore they declare an *absolute* need for specific rules.[27]

We believe that both positions capture elements of truth.

On the one side, indeed, WTO legal system has been able to apply some of its GATT rules – at least the main ones – to the new requirements of digital markets as a whole; on the other, it is also true, as we said in section 2, that Member States themselves are wide aware of the need to develop specific rules for some specific situations, such as data flows, and have drawn up proposals to that effect. The multilateral trading system crisis has slowed down, if not blocked at all, this process, so, adaptations by practice are extremely desirable to avert WTO's irrelevance.

4. *Data flows and services: tech neutrality and a classification issue*

Even more than what happens with the GATT, data protection domestic regulations influence the GATS system.[28]

The latter leaves Member States a greater freedom and discretion than the former: the multilateral system of trade in services, besides a nucleus of general rules applicable to all the Members, as the most favored nation treatment (MFN, Article II) and transparency (Article III), contemplates most penetrating obligations, as national treatment (Article XV) and market access (Article XVII), which apply exclusively to the Members who have explicitly accepted them with regard to specific sectors, listed in their own 'schedules of commitments'.[29]

[27] M Burri, 'The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation' (2017) 51 U California Davis L Rev 65.

[28] S Saluzzo, 'Cross Border Data Flows and International Trade Law the Relationship between EU Data Protection Law and the GATS' (2017) 31 Diritto del commercio internazionale 807.

[29] For an in-depth analysis of GATS rules see see P Picone, A Ligustro, *Diritto dell'Organizzazione mondiale del commercio* (CEDAM 2002) 321 ff; R Wolfrum, P Stoll,

The schedules play a pivotal role in the GATS system, as they allow each Member to specify concretely the level of liberalization guaranteed for every services' sector, distinguishing it by the type of service and the modes by which it is supplied.

These modes are listed in Article I, para 2, lett. *a)* to *d)* GATS, which distinguishes *a)* the cross-border supply, in which is the service to flow from one State to another, *b)* the consumption abroad, in which the service consumer reaches the lender in his Country of origin, *c)* the commercial presence, where a service supplier of one Member establishes a territorial presence in another Member's territory in order to provide a service, *d)* the presence of natural persons, in which the lender just moves to the user's Country.

This mechanism makes it possible to adapt the multilateral trading system to the needs of each Member, which can then proceed to liberalize the tertiary sector to the extent deemed most appropriate. The system is then complemented by specific liberalization obligations for specific sectors (such as, for instance, financial services, air and sea transport, and, as regards the subject of our analysis, telecommunications), governed by a series of Annexes to the Agreement.

Let's also remind that by Article XIV GATS States can waive obligations in order to protect some prevalent interests: it is a mechanism very similar to the one provided for by Article XX GATT but that, compared to the latter, provides a greater rigidity[30]. What is more, Article XIV, lett. *c)* GATS provides for a specific exception pertaining 'the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts': it is in this legal context, therefore, that rules on data processing/protection must be framed.

Again, problematic profiles are connected to the identification of the applicable GATS provisions. There are indeed difficulties in fully distinguishing, in digital cases, the supply modes of the service (Article I), in increased risks of violation of MFN (Article II) and transparency (Article III) principles, and of the rules on regulation and recognition

C Feinaugle (eds), *WTO-Trade in Services (Max Planck Commentaries on World Trade Law)* (Brill 2008).

[30] Note 5 at art XIV GATS provides that 'the public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society'

(Article VI and Article VII). There are also complexities pertaining the application of the exceptions for the protection of privacy and public morality (Article XIV) and, again, difficulties of ensuring effectiveness of market access commitments (including commitments in the field of basic services and telecommunications in value added and on distribution services, Article XVI) and national treatment (Article XVII).

But, as we have seen happening with GATT, also with regard to the GATS system the WTO case-law elaborated some principles that can provide us with a guide to the legal mechanisms that regulate the relations between the multilateral trading system in services and national/regional regulations on treatment of data and their cross-border flows.

In this regard the leading case is *US – Gambling*,[31] the second dispute in the history of the WTO to be totally based on GATS[32] and the first, and until now the only one settled, to be totally focused on the exchange of services via the Internet. The dispute was promoted by Antigua and Barbuda, a small State of the Antilles where the betting industry is flourishing, which asked to check the compatibility with the GATS of provisions of US law which, for various reasons, prohibited collecting of bets or gambling by the Internet.

The dispute contains a sample of the multilateral rules on services that a domestic regulation limiting the cross-border movements of data flows can infringe: the so-called domestic regulations obligation (Article VI, which requires that, in the areas subject to specific commitments, general measures concerning trade in services have to be applied in a 'reasonable, objective and impartial way'); the obligation of liberalization of payments (Article XI, which prohibits the WTO Members to impose restrictions on international capital transfers and payments); the national treatment obligations (Article XVII, which, in the sectors subject to specific commitments, requires Members to grant to the services and service providers of another Member a treatment no less favorable than that accorded to similar national services and national service pro-

[31] *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services* (*US – Gambling*) Report of the Panel WT/DS285/R (10 November 2004), Report of the Appellate Body WT/DS285/AB/R (7 April 2005).

[32] The first dispute settled by the WTO which exclusively concerned the application of the GATS rules is *Mexico - Measures Affecting Telecommunications Services (Mexico - Telecoms)* Report of the Panel WT/DS204/R (2 April 2004).

viders); the market access obligation (Article XVI, which prohibits the adoption of quantitative restrictions on the provision of services).

In *Antigua* both the panel and the AB shed light on points that have a general impact on the application of the GATS to digital services, and that may have an impact on the way the multilateral trading system relates to data protection.

In particular, given the relevance that the GATS connects to the mode in which a service is provided,[33] is of great concern the so-called technological neutrality principle:[34] according to the latter, States should not differentiate the legal discipline of a trade-relevant situation solely on the basis of the means used to carry it out; from this follows the need to interpret the schedules of commitments in a 'tech' key, in order to include the digital services.[35]

Moreover, in a WTO perspective the principle constitutes an adaption of the more general principle of non-discrimination, which imposes that, in the absence of causes justifying a differentiated treatment, analogous situations must be treated in a comparable way and different situations in a different one.

The issue is also intertwined to the principle of digital convergence: the Internet is not a service in itself, indeed, but a vehicle for transmitting data that can relate to the most disparate services (publishing, television, radio, telephony, healthcare, etc.), so the catchphrase 'digital convergence' refers to this capacity of the Net to incorporate completely different contents and tools. Digital technology made possible the fusion of a plurality of different instruments each of one, in its traditional form, is subject to independent and even more different regulations, and this also in terms of the liberalization commitments assumed by the States in the WTO context. In the GATS system this translates into the need to read the schedules of commitments in order to subsume a digi-

[33] The Council for trade in services was aware of the relevance of tech neutrality issue for the GATS system almost twenty years ago, when it was cited within the e-commerce working program; see *Interim Report to the General Council* doc S/C/8 (31 march 1999) <www.wto.org>.

[34] On the issue see J Hojnik, 'Technology Neutral EU law: Digital Goods within the Traditional Goods/Services Distinction' (2017) 25 Intl J L and Information Technology 63.

[35] For a comprehensive analysis of the issue see R H Weber, M Burri, *Classification of Services in the Digital Economy* (Springer, 2012).

tally provided service (which involves the processing and transfer of data) within the categories in there planned, and to identify so the level of commitments specifically undertaken by the States.

In this context, limitations to the transboundary transfers of data can be considered as *direct* restrictions when a service for which the State had made specific commitments *consists* in the same transfer of data (one may think of the case of cloud computing or data storage) or as *indirect* restrictions whenever the ban prevent the performance of the service, for which the data are an unavoidable element (eg, the evaluation of a patient's health status on the basis of his anamnestic data). So, there is to understand whether a data transfer provision that conditions the provision of a web-based service leads to violations of market access commitments.

On this point the *Gambling* case clarified that the cross-border mode referred to in Article I, *a)* GATS includes *all possible means* of providing a service from the territory of a WTO Member State to the territory of another: any commitment to market access taken with reference to this mode of supply implies, unless otherwise specified, the right for suppliers of all the Members to deliver a service through every possible means, including the Internet.[36] In the panel's view, this appears to be the only interpretation compatible with the principle of technological neutrality, widely shared among the Members.[37]

In the same case the AB has also clarified that *every* national measure that *entails* an absolute prohibition of providing a given online service is equivalent to 'zero-limit numerical quotas', a particular form of

[36] Para 6.285 of the Panel report.

[37] See also the Work Program on Electronic Commerce - Progress Report to the General Council, doc S/L/74 of 27th July 1999 para 4, adopted by the Council for trade in services <www.wto.org>: 'It is also the general view that the GATS is technologically neutral in the sense that it does not contain any provisions that distinguish between the different technological means through which a service may be supplied'. It should be also noted here that, in the years, some States (and in particular the United States) have supported the idea to frame the exchange of services by electronic means in the consumption abroad mode, since in these cases the user of the service would 'travel', albeit only virtually, to use an electronic service provided in another country. According to other Members, including the EU, instead, the service, 'produced abroad', would be sent to the recipient via the Internet and would then be provided with the cross-border mode. One may also recall that the concessions made with regard to the mode of consumption abroad are more extensive than those made with regard to cross-border mode.

quantitative restriction which does not allow any foreign supplier on a given market, which are prohibited, in particular, by Article XVI, para 2, lett. *a)* GATS.

This could be the case of transboundary data flows blocking measures, at least in the aforementioned *direct* restrictions, whenever a service *consists* in the transfer of data.

5. *A case study. The EU GDPR and its extraterritorial effects*

Let us now try to read the EU GDPR in the light of the aforementioned WTO case-law criteria, in order to understand how multilateral trade rules can influence the way in which national data processing standards work and whether they can be applied in such a way as not to violate pre-existing international obligations.[38]

In the EU, the right to protection of personal data has become autonomous from the 'traditional' right to privacy, as highlighted by the existence of two autonomous provisions in the Charter of fundamental rights of the EU.[39] Before the entry into force of the Lisbon Treaty, in the absence of any explicit legal basis, the rules on personal data protection were approved pursuant to Article 95 TEC, which contemplated the adoption of harmonization measures aimed at achieving the objectives set forth in Article 14 TEC on completion of the internal market. Following the changes made by the Treaty of Lisbon to the competences of the EU, the current legal basis of the data protection rules EU are represented – except the Article 39 TEU relating to the processing of

[38] S Yakovleva, K Irion, 'The Best of Both Worlds? Free Trade in Services, and EU Law on Privacy and Data Protection' (2016) 2 European Data Protection L Rev 191

[39] The Charter, in addition to art 7, which concerns the protection of privacy, contains the art 8, concerning specifically the right to protection of personal data. In para 1 it recognizes the latter to each and every individual, without any regard, therefore, to the citizenship of the Union. Art 8, para 2, in order to ensure such protection, provides for instrumental obligations and requires respect of the principle of loyalty, and that the processing of data – which must be preceded by the consent of the person concerned or, in any case, find a legal basis – can only take place for specific purposes. the right to data protection implies that of accessing it and obtaining its correction. For a comment see O Pollicino, M Bassini, in R Mastroianni, O Pollicino, S Allegrezza, F Pappalardo, O Razzolini (eds), *Carta dei diritti fondamentali dell'Unione europea* (Giuffré 2017) 132; H Kranenborg, in S Peers, T Hervey, J Kenner, A Ward (eds), *The EU Charter of Fundamental Rights* (OUP 2014) 223.

personal data by the Member States in the exercise of activities falling within the scope of the common foreign and security policy – by Article 16 TFEU, which, after recognizing an individual a general (of 'every person') right to protection of personal data, assigns to the Union the competence to adopt, through the ordinary legislative procedure, rules relating to data processing by the Institutions and bodies of the Union and by the Member States in the exercise of activities falling within the scope of EU law.

In application of these rules, as known, the EU has adopted the GDPR, whose scope is limited to 'personal data', defined in its Article 4 as any information concerning an identified or identifiable natural person. It is considered as identifiable 'the natural person who can be identified, directly or indirectly, with particular reference to an identifier such as the name, a number of identification, location data, an online identifier or one or more characteristic elements of its physical, physiological, genetic, psychological, economic, cultural or social identity'.[40]

So, non-personal data remain out of the scope of the GDPR and its rules limiting transboundary data flows, raising different issues of protection, that we cannot afford here.[41]

It must be underlined that the GDPR is even more relevant for the international legal order because it is meant to produce extraterritorial effects. Its Article 3, entitled 'Territorial scope'[42] and operates as a private international law[43] introverted unilateral conflict rule,[44] as it both

[40] A similar approach was adopted by Directive 95/46/EC, repealed by the GDPR, whose art 2 qualified as 'personal data' 'any information concerning an identified or identifiable natural person' (the 'data subject') and considered identifiable any person who can be identified, directly or indirectly, in particular by reference to an identification number or to a or more specific elements characteristic of his physical, physiological, psychological, economic, cultural or social identity.

[41] On the latter Ruotolo, 'I dati non personali' (n 6) 97.

[42] M Gömann, 'The New Territorial Scope of EU Data Protection Law: Deconstructing a Revolutionary Achievement' (2017) 54 Common Market L Rev 567.

[43] In general on the almost inseparable fusion of public and private international law in the Internet-based contexts see JG Castel, 'The Internet in Light of Traditional Public and Private International Law Principles and Rules Applied in Canada' (2001) 39 Canadian YB Intl L 3; T Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/public International Law Interface' (2008) 19 Eur J Intl L 799; DJB Svantesson, 'The Relation between Public International Law and Private International Law in the Internet Context' (Australian Law Teachers' Association Conference, July 2005, Hamilton, New Zealand) <www.svantesson.org>.

identifies and amplifies the scope of EU law extending it to transnational cases, without never contemplating, at the same time, the possibility of applying the 'foreign' law, ie non-EU Countries' law. Indeed, Article 3, para 1, provides for the applicability of the GDPR to all the processing of personal data carried out as part of the activities of an establishment by a controller in the Union, regardless of whether the processing materially takes place on the territory EU.

There is to remind that Article 3 was drafted in conformity of the principles contained in recital 23 of the DPGR itself, which was drawn up taking into account the case law of the EU Court of Justice, in particular the criteria developed in the *Weltimmo* case.[45]

The recital 23 stipulates that, in order to prevent a natural person from being deprived of the protection he or she has under EU law, it is necessary that the latter regulates the processing of personal data of *every* data subject in the Union, even if the same processing is done by controllers that are not established in the Union, whenever the processing activities are *related* to the supply of goods or services offered in the UE, and this regardless of whether there is a connected payment.

To determine whether there is such an offering of goods or services to data subjects who are in the Union, the recital provides it should be

[44] It must be said that the use of introverted unilateral rules of conflict is nowadays extremely rare in domestic laws and in any case there is a widespread tendency to interpret them bilaterally. For a classic example of such rules, we can recall the art 3, paragraph 3, of the French Civil Code of 1804, which provided for the application of French law concerning the status and ability of persons to French citizens even if domiciled abroad. For a recent use of the category see N Boschiero, B Ubertazzi, in T Kono (ed), *Intellectual Property and Private International Law* (Hart 2012) 735.

[45] Case C-230/14, *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (ECJ, 1 October 2015). In this case, decided under the validity of the directive 95/46, the Court established that in order to identify the law applicable to the processing of personal data, the citizenship of the interested party was irrelevant, and it was instead crucial to understand whether who had done the treatment had an organization and actual and real activity, even if minimal, in one Member State. The Court also clarified that the verification of these requirements falls to national courts which, for this purpose, can take into account various factors, including which the fact, on the one hand, that the activity of the responsible for that processing consists in the management of Internet sites written in the language of the latter and that are, as a consequence, mainly, or wholly, addressed to that Member State and, secondly, that that person has a representative in that Member State, who is in charge of recovering the claims arising from this activity and representing it in the administrative and judicial proceedings relating to the processing of the data.

ascertained whether it is apparent that the supplier envisages offering services to data subjects in one or more Member States in the Union.

Now, whereas the mere accessibility in the Union of a website, of an email address or of other contact details, or the use of a language generally used in the third Country where the supplier is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the EU, may make it apparent that the supplier envisages offering goods or services to data subjects in the Union.[46]

On these basis Article 3, para 2 provides that the GDPR applies to the processing of personal data of data subjects in the Union, carried out by a controller who is not established in the Union, when the processing activities concern *a)* the offering of goods or services to such data subjects in the Union, irrespective of whether a payment of the data subject is required, *b)* the monitoring of their behavior as far as their behavior takes place within the Union.

Paragraph 3 also envisages that the regulation applies to the processing of personal data carried out by a controller not established in the Union, but in a place subject to the law of a Member State by virtue of international law. One may think that the latter provision refers (also) to cases such as the ones of Guyana, Guadalupe, Martinique, Mayotte and Réunion (where French law applies) or Bonaire, Saba and Sint Eustatius (where Netherlands law applies) or, again, the Canaries, where French law is applied. In fact, since in these territories EU law is ap-

[46] These parameters are also strongly influenced by the opinion on applicable law no 8/2010 of the Working Group art 29 (0836-02/10/EN/WP179 adopted on 16 December 2010), which suggested to contemplate specific linking criteria for the cases in which the data controller was established outside the EU territory, in order to ensure that in the case of application of the law of a of the Member States there was a sufficient connection with the territory of the Union and, at the same time, to avoid that the EU territory was used to carry out illegal data processing activities by holders established outside the EU. The Opinion suggested, for such cases, both the criterion of 'targeting', which should lead to the application of the law of the place where are located the people to whom the business of the owner is addressed, and the residual criterion of the 'equipment', which should lead to the application of the law of the place where the processing equipment is located, to be applied only in the case of data relating to non-European subjects or if the holder has no connection with the EU other than to have established his equipment.

plied by its own force, it seems doubtful that they may be among the places 'outside the EU' to which the aforementioned rule aims to extend the application of the GDPR; it is therefore more likely that the provision refers to the case of ships flying the flag of EU Members or to the diplomatic offices of the same Countries outside the EU territory.[47]

All these rules, however, greatly extend the scope of the DPGR and thus make it more likely to contrast with rules of international law, in particular the ones we spoke about so far, especially if we consider that the following Articles 44 and 45, which we will deal with in the following paragraph, set limits and conditions for the cross-border transfer of personal data subject to the regulation.

6. *The GPDR in the WTO ecosystem*

In the light of all the examined caselaw, we can say GDPR surely 'affects trade'. WTO dispute settlement bodies have in fact repeatedly clarified that a national measure falls within the scope of the multilateral trade rules if it has an effect on the matters governed by them.[48]

And even the EU legislator proves to be absolutely aware of this impact, since GDPR recital 101 states that 'flows of personal data to and from countries outside the Union and international organizations are necessary for the expansion of international trade and international cooperation'.

It must also be said that the regulation, at least from a formal point of view, does not appear to be *facially* discriminatory. But the system it builds contains rules which, once applied, may result in an unequal treatment between WTO Members which could jeopardize trade opportunities.

[47] In this sense see both the recital 25 of the regulation ('Where Member State law applies by virtue of public international law, this Regulation should also apply to a controller not established in the Union, such as in a Member State's diplomatic mission or consular post') and the already cited opinion on applicable law no 8/2010 of the Working Group art 29.

[48] 'The use of the term "affecting" reflects the intent of the drafters to give a broad reach to the GATS. The ordinary meaning of the word "affecting" implies a measure that has "an effect on", which indicates a broad scope of application', *European Communities - Regime for the Importation, Sale and Distribution of Bananas* – Report of the Appellate Body WT/DS27/AB/R (adopted 25 September 1997) para 220.

The most likely case (not the only one, though) in which the GDPR could breach the multilateral trading rules occurs whenever personal data of subjects residing within the EU have to be transferred to third Countries in order to perform a trade-relevant transaction:[49] the rules contained into Chapter V of the GDPR ('Transfers of personal data to third countries or international organisations') could indeed operate as non-tariff barriers and restrict the liberalization of international trade.

Article 44, that opens the Chapter, contains a 'general principle for transfers' and provides that, in order to ensure that the level of protection of natural persons guaranteed in the EU is not undermined, any transfer of personal data to a third Country or to an international organization shall take place only if the conditions laid down in the same Chapter are complied.

To this end the fulcrum of the system is the following Article 45, which provides a mechanism according to which the Commission, following a series of verifications, may adopt a decision, called 'adequacy decision', allowing the transfer of personal data relating to subjects residing in the territory of the EU to specific States in which there is an adequate level of data protection, somehow comparable to the one guaranteed in the EU. It is such a decision that may entail a different treatment between different WTO Members: in fact, some of the latter could benefit from an adequacy decision, while others could be banned for the low level of protection of personal data they offer, and this could on cascade imply limitations on trade exchanges also with other WTO Members. And all on the basis of considerations and reasons that are trade-offs, wholly unrelated to the demands of liberalization of international exchanges.

This raises doubts about compatibility of the procedure and the measures with the conditions laid down by the WTO rules for the adoption of exceptions, and in particular, with the rules governing gen-

[49] The EU Court of Justice, in the *Bodil Lindqvist* case (Case C-101/01 [2003] ECR I-12971) has stated that the insertion of personal data on a website by their owner does not constitute transfer of personal data outside the Union even if such data, following the insertion, should be accessible to persons residing outside the Union, if the server on which they are stored is within the Union itself.

eral exceptions such as Article XX GATT and the Article XIV GATS that we have already examined.[50]

On the other side the GDPR eliminates the need to request the competent national data protection authority for an authorization to transfer data abroad, that was instead provided for in directive 95/46; the latter, indeed, was potentially incompatible, with WTO rules relating to administrative authorizations and licenses (such as Article XI GATT). The regulation also provides for the use of codes of conduct or certification schemes (Article 46) to demonstrate the existence of adequate guarantees in the legal order of data destination.

But the authorization of national authorities is still necessary if a data controller wishes to use, in order to transfer data to third countries, *ad hoc* contractual clauses, that is to say clauses not previously recognized as adequate by a Commission decision, or even when a data transfer is to be made by administrative agreements between public authorities.

Furthermore – and this is a very important provision in light of the extraterritorial application we talked about in the previous paragraph – the regulation itself prohibits the transfer of data to third Countries on the basis of judicial decisions or administrative orders issued by the authorities of the latter, unless international agreements have been concluded in this sense (Article 48). Although the provision makes explicit reference only to cooperation agreements in judicial matters, its formulation seems to declare the admissibility of any international agreement aimed at legitimizing the transfer of data: in this sense, therefore, trade agreements that contemplate the transfer of personal data in the context of commercial activities may fit the case.[51]

Finally, Article 49 GDPR provides for derogations for specific situations and permits the transfer of personal data to a third Country that does not respond or does not meet the requirements of adequacy when

[50] See paras 3 and 4. For some analysis of these aspects in under the Directive 95/46 see FM Caklin, 'European Privacy Standards and their Implications for International Trade. The EU Data Protection Directive' (1998) 1 J World Intellectual Property 539; CL Reyes, 'WTO Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive' (2011) 12 Melbourne J Intl L 1.

[51] M Burri 'New Legal Design for Digital Commerce in Free Trade Agreements' (2017) 107 Digiworld Economic J 1; K Irion, S Yakovleva, M Bartl, 'Trade and Privacy: complicated bedfellows? How to achieve data protection-proof free trade agreements' (2016) Amsterdam Institute for Information Law.

a) data subject has explicitly consented to the proposed transfer, after having been informed of the risks of such transfer; *b)* the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; *c)* the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; *d)* the transfer is necessary for important reasons of public interest; e) the transfer is necessary for the establishment, exercise or defence of legal claims; *f)* the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; *g)* the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Even such a rule, indeed, does not seem to make the GDPR system fully compatible with the multilateral trading rules, since it leaves to the will of private individuals the possibility for the EU of respecting international trade obligations.

And this seems even more peculiar if we remind that individuals have no *locus standi* at all in WTO system.

7. *Conclusions*

Although the GDPR has at least relieved some of the most marked elements of incompatibility with the multilateral trading system that affected the EU legal order under the 'old' data directive, it maintains some aspects of conflict with the same system, and therefore may represent an element of restriction of both trade in goods (not only liquid ones) and services, in accordance with the provisions we have examined in paragraphs 2 and 3.[52] And this despite the fact that its Article 49, as

[52] See <itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>.

we have just seen, allows the transboundary transfer of data even in the absence of adequacy decisions or of adequate guarantees, on the assumption of the consent of the interested party or in order to comply with contractual obligations.

The described situation appears as being part of a general trend that, apart from the case of specific derogation provisions, sees most developed States imposing a sort of general prohibition or limitations on the transfer of data abroad, in order to protect some paramount interests of the individuals residing on their territory.

A more relaxed approach, on the other hand, characterizes the developing countries, probably because they aim at attracting data and, by them, investments.[53]

The transfer of data is, on the contrary, allowed and fully legitimate, in the context of regional integration or preferential trade agreements.[54]

This trend, we think, could be read in the context of the progressive reduction of relevance of the multilateral trading system and of the crisis that is striking the WTO, with its fragmentation into legal subsystems.

The described phenomenon, moreover, can be framed in an even broader framework that is seeing information technologies, and in particular those on data processing, influencing the way law works, by modifying also its core values: this is impacting not only on a 'parochial, privacy-fixated formulation of the field of inquiry known as 'law and technology'', but in a wider sense, on the whole international legal order[55] by putting together the dreamy, initiated, approach of IT law and the pragmatic one of international economic law. So data protection rules' impact on WTO system seems to allocate just where dream and day unite.[56]

[53] DA MacDonald, CM Streatfeild, 'Personal data privacy and the WTO' (2014) 36 Houston J Intl L 625.

[54] S Yakoleva, 'Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"?' (2017) 16 World Trade Rev 1; A Bendiek, E Schmeg, 'European Union Data Protection and External Trade' (2016) *SWP Comments* issue 11 <www.swp-berlin.org/en/publication/eu-data-protection-and-external-trade>.

[55] F Johns, Data, Detection and the Redistribution of the Sensible in International Law (2017) AIJL 57.

[56] The reference is to 'Where Dream and Day Unite', a record by the American band Dream Theater, published in 1989 by MCA Records.